U.S. DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FILED
NOV - 6 015
CLERK, U.S. DISTRICT COURT
By TEXAS
Deputy

SEALED

United States District Court

NORTHERN DISTRICT OF TEXAS

In the Matter of the Search of
(Name, address or Brief description of person, property or premises to be searched)

Premises known as:
6109 Bay Island Drive, Apt. 1079
Garland, Texas 75043

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: 3:15-MJ-809-BN

I Robert M. Jester **being duly sworn depose and say:**
I am a(n) Special Agent with the United States Department of Homeland Security (HSI) **and have reason to believe that on the person of or** XX **on the property or premises known as** (name, description and/or location)

(SEE ATTACHMENT A).

in the NORTHERN **District of** TEXAS **there is now concealed a certain person or property, namely (describe the person or property to be seized)**

(SEE ATTACHMENT B).

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)
property that constitutes evidence of the commission of a crime, contraband, the fruits of crime, and is, otherwise, criminally possessed, **concerning a violation of Title** 18 **United States code, Section(s)** 2252 and 2252A. **The facts to support a finding of Probable Cause are as follows:**

(SEE ATTACHED AFFIDAVIT OF SPECIAL AGENT ROBERT M. JESTER).
Continued on the attached sheet and made a part hereof. XX **Yes** __ **No**

Signature of Affiant
ROBERT M. JESTER
Special Agent, HSI

Sworn to before me, and subscribed in my presence

November 6, 2015, 9:58 a.m. **at** Dallas, Texas
Date and Time **City and State**

DAVID L. HORAN
United States Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Robert M. Jester, a Special Agent with the United States Department of Homeland Security (HSI), being duly sworn, depose and state as follows:

1. I am a Special Agent with the United States Department of Homeland Security Investigations (HSI), assigned to the Special Agent in Charge, Dallas, Texas. I have been employed with HSI and its predecessor organization, the Immigration and Naturalization Service (INS), since June 1994. As part of my duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. I have received training in the area of child pornography and child exploitation, and, during investigations, have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have been involved in numerous child pornography investigations and am very familiar with the tactics used by child pornography offenders who collect and distribute child pornographic material.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. This affidavit is being made in support of an application for a search warrant for **6109 Bay Island Drive, Apt. 1079, Garland, Texas 75043**, within the Northern District of Texas, more particularly described in Attachment A, for the items

specified in Attachment B hereto.

4. The purpose of this application is to seize evidence, fruits, and instrumentalities, more particularly described in Attachment B, of violations of 18 U.S.C. §§ 2252 and 2252A, which make it a crime to possess, receive, and/or transport child pornography. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, are presently located at **6109 Bay Island Drive, Apt. 1079, Garland, Texas 75043**, the subject premises.

BACKGROUND REGARDING SEIZURE OF COMPUTERS

5. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that searches and seizures of evidence from computers commonly require agents to seize most of the computer items (hardware, software and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. That is almost always true because of the following:

6. Computer storage devices (like hard drives, diskettes, tapes, laser disks, and others) store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all the stored data to

determine whether it is included in the warrant. This examination process can take weeks or months, depending on the volume of the data stored, and it would be impractical to attempt this kind of data search on-site.

7. Searching computer systems for criminal evidence is a highly technical process requiring expert skills in a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in some systems and applications. It is difficult to know before a search which expert should analyze the system and its data. A search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

8. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as the central processing unit ("CPU"). In cases like this one, where the evidence consists partly of graphic files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover,

searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly retrieve the evidence sought.

9. In addition to being evidence of a crime, in child pornography cases/investigations involving computers, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, printer, modem and other system components were used as a means of committing offenses involving the sexual exploitation of minors in violation of law, and should all be seized on that basis alone. Accordingly, permission is sought herein to seize and search computers and related devices consistent with the scope of the requested search.

BACKGROUND REGARDING THE INTERNET/COMPUTERS AND CHILD PORNOGRAPHY

10. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet

Protocol ("IP") Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing; that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

11. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily,

reproduce it inexpensively, and distribute it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

12. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy or compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 250 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

13. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is

stored in his computer. The process of transporting an image file to one's own computer is called "downloading." The user can then display the image file on his computer screen, and can choose to "save" the image on his computer and/or print out a hard copy of the image by using a printer device (such as a laser or inkjet printer).

14. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a

particular user's operating system, storage capacity, and computer habits.

OVERVIEW OF PEER-TO-PEER CHILD PORNOGRAPHY INVESTIGATION TERMS, BACKGROUND, AND METHODOLOGY

15. Peer-to-peer (P2P) file sharing programs are a standard way of transferring files from one computer system to another while connected to the Internet. P2P file sharing programs allow groups of computers using the same file sharing network, e.g. "Ares," "Gnutella," "eDonkey," to connect directly with each other and to share files from one another's computer systems. Presently, millions of persons throughout the world use P2P file sharing networks to share many types of files among each other. P2P application software allows networked computer users, connected to the Internet, to share many types of files with other users. These files typically include music, graphics, images, movies, and text. In this way, users are able to collect large numbers of files, including child pornography.

16. P2P network software allows individuals to use their computers to exchange files directly over the Internet without having to go through or access a specific website in an arrangement that can be described as computer-to-computer (or person-to-person, hence the name peer-to-peer) connection. Unlike a website, P2P file sharing networks enable persons to obtain files directly from one another as long as they are connected to the Internet. Furthermore, P2P enables an individual to view the files made available to share to other P2P users. Upon installation and enabling P2P software on one's computer, that computer then becomes both a client and a server in the network and

is able to share desired files that have been placed in what is referred to as a "shared folder," on a user's hard drive, with other P2P users. The P2P network has software installed on them that facilitates the trading of images and other files. The software, when installed, allows the user to search for pictures, movies, and other digital files by entering text as search terms. For example, an individual looking for music files by a specific artist may enter a search term such as "Tupac," and will receive nearly instantaneously a list of other P2P users that have music titles pertaining to rap music artist, Tupac Shakur, on their hard drives that have been made available to others on the network.

17. Because of its relative ease of use and perceived anonymity, P2P networks provide readily available access to child pornography. As a result, law enforcement officers/agents throughout the United States have participated in Internet undercover operations to identify persons using P2P software on the Internet to traffic in child pornography. These law enforcement officers/agents know from using the various P2P networks that users can find images and movies of child pornography by using search terms like "babyj." The "babyj" search term typically results in the user being presented with a listing of files that include movies of a known child from Georgia being vaginally penetrated by an adult male.

18. It is known from using the various P2P software that the search results presented to the user allow the user to select a file and then receive that file from other users around the world. Often these users can receive the selected movie from numerous

sources at once. The software can balance the network load and recover from network failures by accepting pieces of the movie from different users and then reassembling the movie on the local computer. It is possible to have, and some P2P software platforms require, a single source download in addition to the numerous source download. However, a single source download is often slower and less efficient than a multiple source download.

19. I know that the P2P file sharing network can only succeed in reassembling the movie from different parts if the parts all come from the exact same movie. I know that multiple persons sharing one movie can deliver pieces of that movie to the local software and the local software can insure a complete and exact copy can be made from the parts. Agents have been able to confirm through use of the software that the different copies of the same movie may have different file names.

20. Pursuant to this investigation, I know from training and experience that Internet computers identify each other by an Internet protocol (IP) address. I know that these IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead the law enforcement officer to a particular ISP company and that company can typically identify the account that uses the IP address to access to the Internet.

21. Pursuant to this investigation, I have been able to capitalize on the Internet's and P2P network's reliance on IP addresses to geographically locate computers within the Northern District of Texas that have made known images and/or movies of

child pornography available for distribution via P2P file-sharing. This specificity to a geographic location via IP address has been made possible through the utilization of software that enables investigators to categorize IP addresses by geographical parameters.

22. It should be noted that the software developed merely categorizes by general geography IP addresses that have been broadcast by a suspect's own computer onto the network as a function of the network software. Because the software developed does not provide any additional identifying data other than a user's IP address, it is incumbent upon investigating officers/agents to take additional steps toward the identification and specific location of the computer that is being used to distribute child pornography. It should be further noted that the ability to view the file names and/or SHA-1 values a suspect has on his computer is a direct function of the P2P file-sharing software that the suspect has freely and independently utilized in furtherance of his file-sharing activities, and is not a function of any software designed by or proprietarily utilized by law enforcement. Simply stated, by definition, the suspect himself has in effect advertised publicly, via the Internet, which files he has on his hard drive by making those files available to P2P network users nationally and internationally. Law enforcement agents/officers have simply availed themselves of this information by accessing the network in the same fashion that any private individual is able to do.

23. Based on the foregoing, I, along with other participating law enforcement agencies, initiated an investigation concentrating on the identification of computers and persons located within the Northern District of Texas that are distributing images and/or

movie files of child pornography via the Internet through the utilization of P2P file-sharing software.

BACKGROUND OF THE INVESTIGATION

24. From September 12, 2015 until October 5, 2015, Garland, Texas Police Detective Tony Godwin was conducting investigations into the sharing of child pornography files on a Gnutella P2P file sharing network.

25. On September 12, 2015, Detective Godwin directed his investigative focus to a device with the IP address 173.175.219.209 because it reported at least 1 file being shared which was indicative of child pornography.

26. Using a computer running investigative software, Detective Godwin directly connected to the device at IP address 173.175.219.209. This device reported itself as WinMX Music/6.3.0, GUID 905FD0D8CDE8D55CCCD2965DF90EE600. The GUID, which is an acronym for Globally Unique Identifier, is a 128-bit number that is produced by many computer applications, including Gnutella P2P file sharing networks, to uniquely identify a particular user.

27. Between September 12, 2015 at 0436 UTC-5:00 and October 5, 2015 at 0307 UTC-5:00, Detective Godwin downloaded 4 files suspected of containing child pornography from the sharing client who had the IP address 173.175.219.209, which were recorded along with the date, time, and hash value of each file transfer. Three of these files are listed below:

File Name	File Description
(Pthc) 10 yo fuck and cum all over her – 3.mpg	This 2-minute, 59-second video depicts a prepubescent girl, completely nude, lying on her back on a bed. An adult male is shown penetrating the girl's vagina with his penis. The adult male then ejaculates onto the girl's back, then penetrates the girl's anus with an object and his penis.
__Pthc - !!New!! 2004 Cum Mouth And Face Very Good Avi.----Mpg--, 3Yr, 4Yr, Lolita, Hussyfat, Open, Tug, Dvd, Uu,--, Childlover, Pedo.avi	This 10-minute, 40-second video is a compilation of three different prepubescent girls, all completely nude, performing oral sex on adult males.
(Pthc) – 8Yr Little Cuty Ass Raped B.mpg	This 1-minute, 5-second video depicts a prepubescent girl, age 6-8, completely nude, lying on a bed with a towel covering her eyes. An adult male is shown rubbing his erect penis against the girl's vagina.

28. These files were downloaded using a single-source program, meaning that all files were completely downloaded only from the computer at IP address 173.175.219.209.

29. Subsequent to these downloads, I conducted a query on the IP address 173.175.219.209 through the American Registry for Internet Numbers (ARIN) and obtained information that the target IP address was registered to Internet Service Provider (ISP) Time Warner Cable.

30. On October 13, 2015, Agent Jester sent an administrative summons to Time Warner Cable requesting subscriber information for the IP address 173.175.219.209 that was logged on the dates of September 12, 2015 at 0436 UTC-5:00 through October 5, 2015 at 0307 UTC-5:00.

31. On October 28, 2015, Time Warner Cable responded to the summons.

According to Time Warner Cable's records, the subscriber using IP address 173.175.219.209 on those dates and times was Zack ZENISEK at the address 6109 Bay Island Drive, Apt. 1079, Garland, Texas 75043. The account was created on July 16, 2015 and was still active as of the date of the summons.

32. The CLEAR public information database lists 6109 Bay Island Drive, Apt. 1079, Garland, Texas 75043 as a recent address for Zachary ZENISEK. The report also lists a 2011 Chevrolet Camaro, bearing Texas license FWR 9974 as being registered to ZENISEK.

33. On October 28, 2015, Agent Jester conducted surveillance at 6109 Bay Island Drive, Garland, Texas 75043, which is the Bay Island Apartment Complex. Agent Jester observed the grey 2011 Chevrolet Camaro, bearing Texas license FWR 9974, parked at the complex. Agent Jester spoke with the Manager of the apartment complex, who verified that ZENISEK and his roommate Daniel Trafton was currently residing in apartment 1079 and that they had been residing in the apartment since July 2015.

34. Based on the aforementioned factual information, I believe that there is probable cause to believe that an individual who resides at the subject premises is involved in the possession, transportation and distribution of child pornography in violation of 18 U.S.C. §§ 2252 and 2252A. Additionally, there is probable cause to believe that evidence and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, are located at the subject premises at **6109 Bay Island Drive, Apt. 1079, Garland, Texas 75043** and this evidence, listed in Attachment B, constitutes

instrumentalities and evidence, which is or has been used as the means of committing the foregoing offenses.

35. I therefore respectfully request that the attached warrant be issued authorizing the search of the premises described in Attachment A, and seizure of the items listed in Attachment B.

ROBERT M. JESTER
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 6th day of November, 2015 at 9:50 a.m.

DAVID L. HORAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
DESCRIPTION OF THE PREMISES TO BE SEARCHED

This warrant applies to the premises located at **6109 Bay Island Drive, Apt. 1079, Garland, Texas 75043** in the Northern District of Texas. The premises is an 1184 square foot, two-bedroom apartment within the Bay Island apartment complex.

The search is to include all rooms, attics, basements, and all other parts therein, and surrounding grounds, garages, storage rooms, or outbuildings of any kind, attached or unattached, located on the premises relating to the premises. The search also includes the search of vehicles located at or near the premises, which fall under the dominion and control of the person or persons associated with the premises. The search of those vehicles is to include all internal and external compartments and all containers that may be associated with the storage of child pornographic materials or their instrumentalities contained within the aforementioned vehicles.

ATTACHMENT B
DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

1. Computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Evidence of who used, owned, or controlled the computer(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, accounts of Internet Service Providers.

3. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence, rental or lease agreements, mortgage documents, rental or lease payments and credit card information, including, but not limited to, bills and payment records.

4. Any and all notes, documents, records, computer files or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail

messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), including communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography or membership in online groups, clubs, or services that provide or make accessible child pornography to members; .

5. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

6. Any and all cameras, film, videotapes or other photographic equipment.